Amendments to the claims:

This listing will replace all prior versions and listings of claims in this application:

Listing of claims:

Claim 1. (currently amended) ~~A~~An improved method of~~for~~ maintaining privacy for transactions ~~comprising~~ employing a user device having a security module, wherein the improvement comprises the steps of: ~~having a security module with a privacy certification authority computers and a verification computer, the verification computer having obtained public keys from the privacy certification authority computer and from an issuer that provides attestation of the security module, the method further comprising the steps of:~~

~~receiving a first and second set of attestation-signature values, the first set of attestation-signature values being generated by the user device using first attestation values obtained from the issuer and the second set of attestation-signature values being generated by the user device using second attestation values obtained from the privacy certification authority computer;~~

~~checking the validity of the first set of attestation-signature values with the public key of the issuer;~~

~~checking the validity of the second set of attestation-signature values with the public key of the privacy certification authority computer ;and~~

~~verifying whether or not the first and second sets of attestation-signature values relate to the user device.~~

receiving at a verification computer a first set of signature values generated by the user device using a first set of values obtained from an issuer;

receiving at the verification computer a second set of signature values generated by the user device using a second set of values obtained from a privacy certification authority computer;

checking at the verification computer the validity of the first set of signature values with a public key of the issuer;

checking at the verification computer the validity of the second set of signature values with a public key of the privacy certification authority computer; and

verifying a proof at the verification computer that the first and second sets of signature values are based on the first and second sets of values that are obtained from a common value that is unique to the user device;

wherein the privacy certification authority computer uses a same base value for a sufficiently long period of time such that the privacy certification authority computer can determine a frequency with which the security module has requested certification, thereby allowing the privacy certification authority computer to identify whether the security module is a rogue security module.

Claim 2. (currently amended) The improved method according to claim 1, wherein the step of verifying comprises the step of:

verifying that a first value is derived from a base value~~, comprised~~ included in the first set of ~~attestation~~ signature values, ~~and~~ is identical~~to~~ with a second value that is ~~derived~~ obtained from ~~said~~ the base value, and is ~~comprised~~ included in the second set of ~~attestation~~ signature values~~1~~.

Claim 3. (canceled)

Claim 4. (currently amended) The improved method according to claim 2, wherein the base value is different each time the method is applied.

Claim 5. (currently amended) The improved method according to claim ~~3~~1, wherein the common value is obtained~~derived~~ from an endorsement key that is related to the security module.

Claim 6. (withdrawn) A method for maintaining privacy for transactions comprising employing a user device having a security module with a privacy certification authority computer and a verification computer, the privacy certification authority computer having obtained a public key from an issuer that provides attestation of the security module; the method further comprising the steps of:

receiving an initial set of attestation-signature values (DAA1') from the user device, the initial set of attestation-signature values (DAA1') being generated by the user device using first attestation values obtained from the issuers;

checking the validity of the initial set of attestation-signature values with the public key of the issuer;

responsive to the checking step issuing second attestation values that relate to the initial set of attestation-signature values (DAA1'); and

providing the second attestation values to the user device, a second set of attestation-signature values being derivable from the second attestation values, wherein it is verifiable that a first set of attestation-signature values and the second set of attestation-signature values relate to the user device, the first set of attestation-signature values is generatable by the user device using first attestation values obtained from the issuers.

Claim 7. (withdrawn) The method according to claim 6, wherein the step of issuing the second attestation values further comprises the step of:
receiving a request value from the user device and verifying whether the request value relates to the initial set of attestation-signature values.

Claim 8. (withdrawn) A method comprising maintaining privacy for transactions performable by a user device having a security module with a privacy certification authority computer and an verification computer, the user device having obtained first attestation values from an issuer and second attestation values from the privacy certification authority computer, the method step of maintaining comprising the steps of:

generating a first set of attestation-signature values by using the first attestation values and a second set of attestation-signature values by using the second attestation values ;and

sending the first and second set of attestation-signature values to the verification computer, wherein the verification computer is able to check the validity of the first set of attestation-signature values with an issuer public key (PK.sub.I) of the issuer, the validity of the second set of attestation-signature values with an authority public key (PK.sub.PCA) of the privacy certification authority computer and to verify that the first and second sets of attestation-signature value relate to the user device.

Claim 9. (withdrawn) The method according to claim 8, wherein the step of generating comprises using an endorsement key that is related to the security module.

Claims 10 - 11. (canceled)

Claim 12. (withdrawn) A system for maintaining privacy while computers performing transactions comprising:

an issuers providing an issuer public key (PK.sub.I);

a user device having a security module for generating a first set of attestation-signature values;

a privacy certification authority computer for providing an authority public key (PK.sub.PCA) and issuing second attestation values; and

a verification computer for checking the validity of the first set of attestation-signature values with the issuer public key (PK.sub.I)and the validity of a second set of attestation-signature values with the authority public key (PK.sub.PCA), the second set of attestation-signature values being derivable by the user device from the second attestation values, wherein it is verifiable that the first and second sets of attestation-signature values relate to the user device.

Claim 13. (withdrawn) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing maintenance of privacy for transactions, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 6.

Claim 14. (withdrawn) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for maintaining privacy for transactions, said method steps comprising the steps of claim 6.

Claim 15. (withdrawn) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing maintenance of privacy for transactions, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 8.

Claim 16. (withdrawn) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for maintaining privacy for transactions, said method steps comprising the steps of claim 8.

Claim 17. (withdrawn) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing maintenance of privacy for transactions, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 12.

Claims 18 - 20. (canceled)

Claim 21. (new) The improved method of claim 1, wherein the common value is not forwarded to the security module in the user device.

Claim 22. (new) The improved method of claim 1, wherein the privacy certification authority computer does not learn any useful information about the common value.

Claim 23. (new) The improved method of claim 1, wherein the user device can use the second set of values only once and only with a given verifier.

Claim 24. (new) A computer program product tangibly embodying computer readable instructions which when executed causes the computer to implement the steps of the improved method of claim 1.